



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|--------------------------------------|------------------------|
| 10/759,799 | 01/15/2004 | Hemant Kumar Jain | INT-102/US | 8270 |
| 30869 7590 01/07/2008 LUMEN PATENT FIRM, INC. 2345 YALE STREET SECOND FLOOR PALO ALTO, CA 94306 | | | EXAMINER SHAIFER HARRIMAN, DANT B | |
| | | | ART UNIT 2134 | PAPER NUMBER |
| | | | MAIL DATE 01/07/2008 | DELIVERY MODE PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/759,799

Applicant(s)

JAIN, HEMANT KUMAR

Examiner

Dant B. Shaifer - Harriman

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 November 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 - 3, 8 - 10, 21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1 - 3, 8 - 10, 21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

DETAILED ACTION

Response to Amendment

- Claims 4 – 7 & 11 - 20 are cancelled.
- Claims 1, 21 are amended.
- Claims 2, 3, 8, 9, 10 are original.
- Objection on the Specification concerning the labeling of "Multicast Flood Meter 604," has been withdrawn in light of the applicant's correction.

Response to Arguments

Applicant states: *"However, in paragraph 0079 Malan merely mentions the use of an access control list (ACL) as a filter mechanism, but does not teach that the ACL contains IP addresses which have established valid TCP connections, or adding an IP address to the ACL when the TCP state transitions."*

- Examiner respectfully disagrees, in paragraph 0079 of Malan, the examiner notes that the routing system uses a an ACL or access control list, that is used to filter out unwanted attempts gain access to the computer system, to one of ordinary skill in the art, one would know that a data packet contains a source and destination IP or internet protocol addresses, thus the ACL contains a record of legitimate IP address that will be allowed to access the computer system, the examiner interprets " *IP addresses which have established valid TCP connections,*"

merely as a user who connects to the network thru their perspective ISP or internet service provider, and request access to the computer system that employs an ACL to filter unwanted attempts to access the computer system resources, furthermore the examiner notes that the examiner interprets " or adding an IP address to the ACL when the TCP state transitions ," merely as a user logging on (i.e. TCP transition) to the internet and making an unwanted attempt to gain access to the computer system's resources, and the computer system reacts by adding the user's IP address that made the illegal attempt to gain access to the computer system's resources to the other ACL's, to prevent the further penetration into the computer system's resources in the computer system, please see paragraph 0086.

Applicant states: *"Cited paragraph 0073 of Malan relates to the processing of alert messages; it does not relate to an ACL and does not teach that the ACL contains IP addresses which have established valid TCP connections, or that an IP address is added to the ACL when the TCP state transitions. "*

- Examiner respectfully disagrees, the Zones X, Y contain the routers which employ ACL's, furthermore, in paragraph 0079 of Malan, the examiner notes that the routing system uses a an ACL or access control list, that is used to filter out unwanted attempts gain access to the computer system, to one of ordinary skill

in the art, one would know that a data packet contains a source and destination IP or internet protocol addresses, thus the ACL contains a record of legitimate IP address that will be allowed to access the computer system, the examiner interprets " *IP addresses which have established valid TCP connections,*" merely as a user who connects to the network thru their perspective ISP or internet service provider, and request access to the computer system that employs an ACL to filter unwanted attempts to access the computer system resources, furthermore the examiner notes that the examiner interprets " *or adding an IP address to the ACL when the TCP state transitions ,*" merely as a user logging on (i.e. TCP transition) to the internet and making an unwanted attempt to gain access to the computer system's resources, and the computer system reacts by adding the user's IP address that made the illegal attempt to gain access to the computer system's resources to the other ACL's, to prevent the further penetration into the computer system's resources in the computer system, please see paragraph 0086.

Applicant states: "*Cited paragraph 0065 of Malan describes components of a collector; it does not discuss an ACL and does not teach the use of an ACL containing IP addresses which have established valid TCP connections, or that an IP address is added to the ACL when the TCP state transitions. Moreover, no other portion of Malan teaches these claimed limitations.*"

- Examiner respectfully disagrees, the collector is a part of the router which employs ACL's, furthermore, in paragraph 0079 of Malan, the examiner notes that the routing system uses a an ACL or access control list, that is used to filter out unwanted attempts gain access to the computer system, to one of ordinary skill in the art, one would know that a data packet contains a source and destination IP or internet protocol addresses, thus the ACL contains a record of legitimate IP address that will be allowed to access the computer system, the examiner interprets " *IP addresses which have established valid TCP connections,*" *merely* as a user who connects to the network thru their perspective ISP or internet service provider, and request access to the computer system that employs an ACL to filter unwanted attempts to access the computer system resources, furthermore the examiner notes that the examiner interprets " *or adding an IP address to the ACL when the TCP state transitions,*" *merely* as a user logging on (i.e. TCP transition) to the internet and making an unwanted attempt to gain access to the computer system's resources, and the computer system reacts by adding the user's IP address that made the illegal attempt to gain access to the computer system's resources to the other ACL's, to prevent the further penetration into the computer system's resources in the computer system, please see paragraph 0086.

Applicant states: *"However, Goldstone does not teach the specific claimed feature of maintaining a list of legitimate IP addresses that contains IP addresses which have established valid TCP connections, or the specific claimed feature of adding an IP address to the list when the TCP state transitions. Goldstone, therefore, does not teach the claimed limitations."*

- Examiner respectfully disagrees, when Goldstone and Malan is combined, applicants invention is obtained, for further reasoning please see examiner's response to applicants arguments above.

Applicant states: *"Applicant respectfully disagrees with certain aspects of the recent Action upon which the rejections were based. For example, regarding the claimed limitation of classifying the received packets according to network layer 2, 3, 4 classification, the Action cites paragraph 0067 of Malan and alleges that, to one of ordinary skill in the art, the collector of Malan will collect routing information of packets "such as what layers the data packet must take in order to get to its destination." This argument, however, merely establishes that it is known in the art for packet routers to process various network layers for routing purposes. This argument does not support the allegation that Malan combined with knowledge of one of ordinary skill in the art teaches or suggests the specific claimed feature of classifying packets according to network layer 2, 3, 4 classification. Routing does not necessarily or inherently involve*

packet classification, nor does it specifically involve classification by network layers 2, 3,

4. This claimed feature, therefore, is not taught in the prior art."

- Examiner respectfully disagrees, to one of ordinary skill in the art, a data packet contains a source and destination IP address, that dictates where the data packet came from and is going to, furthermore the examiner notes that the network layer 2 is called "Data link layer," and that network layer 3 is called "network layer," and that network layer 4 is actually called "transport layer," according to the OSI or Open systems Interconnection Basic Reference Model, furthermore the examiner notes that applicant overlooked that to an ordinary person skilled in the art would realize that when for example that data packets are sent from a source to a destination, the data packet must pass through the various layers of the OSI model in order for the data or information to be transported and processed in systematic and efficient manner or protocol.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim(s) 1- 3 & 8 – 10 & 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (US PGPUB # 2002/0032871) in view of Goldstone (US PGPUB # 2002/01011819).

Malan discloses a method and system for detecting, tracking and blocking denial of service attacks over a computer networks:

- Media access controller (MAC) interface (a controller which is coupled to the collector, the controller is constructed and arranged to receive and respond to the plurality of signals by tracking attributes related to the one or more data packet flow anomalies to at least one source, the controller is further constructed and arranged to block the one or more data packet flow anomalies using one or more filtering mechanisms executed in close proximity to the at least one source; filtering mechanisms can include a plurality of filter list entries, such as access control list entries as well as firewall filter entries, and/or a plurality of rate limiting entries, Paragraph: 0079, 0073, 0065, the examiner notes that to one of ordinary skill in the art, a firewall filter entry list, or access control list will have a table of legitimate IP address to accept and or a list of illegitimate IP addresses that the firewall isn't to accept.);
- Classification means for classifying data packets according to layer2, layer3, layer4 (the collector also includes a buffer, which is adapted to receive and process the plurality of data statistics to generate at least one record that is

communicated to the profiler, Paragraph: 0067, the examiner notes that to one or ordinary skill in the art, all packets must contain data (i.e. source/destination address) and most importantly routing information such as what layers the data packet must take in order to get to its destination, the collector will collect this information for packet routing purposes);

- Meter means for maintaining statistics of attacks, and determining whether a threshold has been reached (a collector interface adapted to receive a plurality of data statistics from the computer network and to process the plurality of data statistics to detect one or more data packet flow anomalies and to generate a plurality of signals representing the one or more data packet flow anomalies Paragraph: 0066, 0084, 0065);
- Decision multiplexer able to receive decisions from meter means, and capable of informing the Media access controller (MAC) interface of a single decision regarding the data packet statistics (the profiler also includes a database for storing a plurality of data packet flow profiles and related information; a detector is adapted to receive and process the predetermined threshold and the at least one record to detect if attributes associated with the record exceed the predetermined threshold, which represents the one or more data packet flow anomalies, Paragraph: 0084, the examiner notes that the profiler is the multiplexer and the MAC is the zone controller or local controller);

- A source tracking mechanism that multiplicatively incrementing the count for sources that send identified flood data, thereby distinguishing sources from others that send non-flood data (the controller is constructed and arranged to receive and respond to the plurality of signals by tracking attributes related to the one or more data packet flow anomalies to at least one source, the controller is further constructed and arranged to block the one or more data packet flow anomalies using one or more filtering mechanisms executed in close proximity to the at least one source; filtering mechanisms can include a plurality of filter list entries, such as access control list entries as well as firewall filter entries, and/or a plurality of rate limiting entries Paragraph: 0079, 0073, 0065, the examiner notes that the controller is able to keep track of the various sources that may send flood data or non-flood data through the profiler and collector utilizes, as they keep track of the statistic associated with the plurality of data packets received by the network resources (i.e. computer or server));
- A SYN flood detection and prevention mechanism have a support means for creating a plurality of legitimate IP addresses during normal operation when the TCP state transitions to Established, where the SYN flood detection and prevention mechanism allows only the plurality of legitimate IP address to be stored during normal operation (the controller is further constructed and arranged to block the one or more data packet flow anomalies using one or more filtering

mechanisms executed in close proximity to the at least one source; filtering mechanisms can include a plurality of filter list entries, such as access control list entries as well as firewall filter entries, and/or a plurality of rate limiting entries, Paragraph: 0079, 0073, 0065, the examiner notes that to one of ordinary skill in the art, a firewall filter entry list, or access control list will have a table of legitimate IP address to accept and or a list of illegitimate IP addresses that the firewall isn't to accept);

- A means for determining a threshold for said connections based on baseline traffic learned during normal operation (a profiler processes the record to generate a predetermined threshold which communicates to the detector (Paragraph: 0068), the profiler also includes a database for storing a plurality of data packet flow profiles and related information; a detector is adapted to receive and process the predetermined threshold and the at least one record to detect if attributes associated with the record exceed the predetermined threshold, which represents the one or more data packet flow anomalies Paragraph: 0084);
- Detection of a SYN flood Dos attacks (Paragraph: 0084, the examiner notes that the storm detector is able to recognize a SYN flood DOS attack based on comparing whether or not a threshold with respect to SYN packet has been exceeded.);

- The rate based denial of service attacks are to an end node or from said end node to other end nodes on the internet (The system for detecting, tracking, blocking of DOS occurs from one computer to another computer on different computer networks, Paragraph: 0057);
- Receiving packets from a network (The system for detecting, tracking, blocking of DOS occurs from one computer to another computer on different computer networks, Paragraph: 0057);
- Creating and storing a table of legitimate IP addresses during normal operation when a TCP state transitions to established (Paragraph: 0079, 0080, the examiner notes that the controller is able to look at other network resources and or routing configurations (i.e. IP addresses of incoming data), and compile or create a list of legitimate address or illegitimate addresses, that will be used to filter out malicious variants of DOS attacks.) furthermore, (the controller also includes a includes a correlator which is used to generate an anomaly table including the attributes related to the one or more data packet flow anomalies Paragraph: 0074, 0086, the examiner notes that to one of ordinary skill in the art, the most common way to track a malicious data packet is by identifying the data packets source address);

- Detecting a SYN flood state (Paragraph: 0084, the examiner notes that the storm detector is able to recognize a SYN flood DOS attack based on comparing whether or not a threshold with respect to SYN packet has been exceeded);

Malan fails to teach a:

- zombie flood detection and prevention mechanism having a means for limiting connections said plurality of legitimate IP addresses stored during normal operation;
- An ager means capable of timing out flood states identified by classification means or meter means, and ager is able to continuously learn, monitor and update statistics;

However, Goldstone discloses a conventional approach to preventing DOS (denial of service) attacks:

- Detection of a Zombie flood (The attacking client's DOS event is initiated when an otherwise legitimate client IP address that has been spoofed by a attacking client, initiates a connection to a network server multiple times to cause congestion to the server or network, this multitude of connection attempts to connect to the server causes congestion or a flood which in fact is a Zombie flood. Zombie floods are caused by clients who initiate connection to the internet

multiple times with a legitimate IP address that will not be blocked by the security entities (i.e. routers, firewalls) of the network or internet, the multiple connection request to the network server causes congestion or a flood, which will not allow other users of the network to request connection through that particular server to logon to the internet until a the timing session for each request to logon to the internet, times out (Paragraph: 0045, 0046, 0050);

- An ager for timing out of a flooding event (Zombie floods are caused by clients who initiate connection to the internet multiple times with a legitimate IP address that will not be blocked by the security entities (i.e. routers, firewalls) of the network or internet, the multiple connection request to the network server causes congestion or a flood, which will not allow other users of the network to request connection through that particular server to logon to the internet until a the timing session for each request to logon to the internet, times out (Paragraph: 0045, 0046, 0050);

Malan and Goldstone are analogous art because they are from the "same field of endeavor," which is the field of detecting, tracking, blocking or preventing "denial of service attacks," or data packet floods moreover, specifically SYN (Synchronization) floods, and Zombie floods.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Malan and Goldstone before him or her, to modify the detection,

tracking, blocking, of a DOS attacks of Malan to include the prevention of a Zombie flood DOS attack of Goldstone, because it would allow for more efficient security coverage or protection of a network, if the DOS attack on the target server or network is initiated from spoofed legitimate address instead of a known illegitimate attacker address.

The suggestion/motivation for doing so would have been to enabled a network that contains security entities (i.e. routers, firewalls), to detect, track, block viruses (i.e. zombie flood attacks) that come from legitimate IP addresses that would otherwise be authorized access to the internet through the target server an continue in attacking the network through multiple internet access requests; to detect a zombie like flood originating from a spoofed legitimate address, Paragraph: 0056 of Malan and Paragraph: 0038 of Goldstone, **please also see KSR International Co. v.Teleflex Inc., 550 U.S. - , 82 USPQ2d 1385 (2007) for further interpretation.**

Therefore it would have been obvious to combine Goldstone with Malan to obtain the invention as specified in the instant claim(s).

Conclusion

Application/Control Number:
10/759,799
Art Unit: 2134

Page 16

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dant B. Shaifer - Harriman whose telephone number is 571-272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

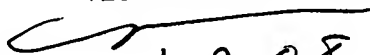
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

12/ 27/2007

D.S.H

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


1/2/08